Customer No. 24498
Attorney Docket No. PD030108
Office Action Date: 03/24/2009

IN THE CLAIMS

Please amend the claims as follows:

1.   (Currently Amended) Method for decrypting data within a <u>playback</u> device, the data comprising an encrypted first data set <u>being audio-visual presentation data</u> and an encrypted second data set <u>being audio-visual supplementary data relating to the first data set</u>, wherein said first data set and at least two respective device independent electronic decryption key are stored on a removable prerecorded storage medium, and the second data set is not stored on the removable prerecorded storage medium but <u>on a second data source and</u> is related to the first data set, <u>the second data source having a first data block that is public, a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the removable prerecorded storage medium</u>, the method comprising the steps of

-    retrieving the first data set and the device independent decryption keys from the removable storage medium;

-    retrieving the second data set from ~~a~~ <u>the second data block of the</u> second data source;

-    decrypting the first data set using a first of said decryption keys; and

-    decrypting the second data set using a second of said decryption keys <u>that are different from the first of said decryption keys</u>, ~~wherein the second decryption key is not used for decrypting the first data set~~.

2.   (Previously Presented) Method according to claim 1, further comprising the step of determining from a plurality of data sets on the second data source a second data set that refers to the removable storage medium, wherein the data sets refer to different removable prerecorded storage media.

3.   (Previously Presented) Method according to claim 1, further comprising the step of detecting whether the removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as authorized

Customer No. 24498
Attorney Docket No. PD030108
Office Action Date: 03/24/2009

if it can be decrypted by said second decryption key.

4.   (Previously Presented) Method according to claim 1, wherein the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains said electronic decryption keys is readable.

5.   (Currently Amended) Apparatus for decrypting data within a playback device, the data comprising an encrypted first data set being audio-visual presentation data and an encrypted second data set being audio-visual supplementary data relating to the first data set, wherein said first data set and at least two respective device independent electronic decryption keys are stored on a removable prerecorded storage medium, and the second data set is not stored on the removable prerecorded storage medium but on a second data source and is related to the first data set, the second data source having a first data block that is public, a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the removable prerecorded storage medium, the apparatus comprising

- means for retrieving the first data set and the device independent decryption keys from the removable storage medium;
- means for retrieving the second data set from the second data block of the a second data source;
- means for decrypting said first data set using a first of said decryption keys; and
- means for decrypting said second data set using a different second of said decryption keys, wherein the second decryption key is not used for decrypting the first data set.

6.   (Previously Presented) Apparatus according to claim 5, further comprising means for determining from a plurality of data sets on the second data source a second data set that refers to the removable storage medium, wherein the data sets refer to different removable prerecorded storage media.

7.   (Previously Presented) Method according to claim 1, wherein the first electronic decryption key is the only suitable key for decrypting the first data set, and the second decryption key is one of several suitable keys for decrypting the second data set.

8.   (Cancelled)

9.   (Previously Presented) Method according to claim 1, wherein the first and second data sets are encrypted using RSA (Rivest-Shamir-Adelman) coding.

10.   (Previously Presented) Apparatus according to claim 5, further comprising means for detecting whether the removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as authorized if it can be decrypted by said decryption key.

11.   (Previously Presented) Apparatus according to claim 5, wherein the first electronic decryption key is the only suitable key for decrypting the first data set, and the second electronic decryption key is one of several suitable keys for decrypting the second data set.

12.   Apparatus according to claim 5, wherein only encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered.

13.   (New) Apparatus according to claim 5, wherein the specified group of removable storage media comprises media that are provided by a particular provider.

14.   (New) Method according to claim 1, further comprising the steps of retrieving a third data set from the third data block, and decrypting the third data set using the second of the decryption keys.

13-15. (New) Method according to claim 1, wherein only encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered.

16. (New) Method according to claim 1, wherein the specified group of removable storage media comprises media that are provided by a particular provider.